Solutions of the Congrunces $x^2 + y^2 \equiv 0\ (mod\ p)$, $x^2 - y^2 \equiv 0\ (mod\ p)$, and $x^4 - y^4 \equiv 0\ (mod\ p)$ for a Prime Number p

Ali Astaneh,PD(Lon), Vancouver BC, Canada

This article might as well have been entitled "Solutions of the Diophantine equations $x^2 + y^2 = pz$, $x^2 - y^2 = pz$, and $x^4 - y^4 = pz$ for prime p", in which case a solution would consists of a pair of integers (x,y) and another integer z depending on x and y. For example, in the straightforward case of $p = 2$ and for the first equation $x^2 + y^2 = pz$; all solutions can be described as all ordered pairs (u,v) of integers, where u and v are either both odd, or they are both even. Then z would be the integer $z = \frac{1}{2}(u^2 + v^2)$.
However, in the congruency versions as stated in the title, a solution will consist of a pair of congruency classes $([u],[v])\ (mod\ p)$ defined by $[u] = \{u + mp\ ,\ m \in \mathbb{Z}\}$ and $[v] = \{v + np\ ,\ n \in \mathbb{Z}\}$ where u and v are certain integers from the least non-negative residues $0, 1, 2, \dots, \mathrm{p} - 1\ (mod\ p)$. More precisely, by a class congruency $(mod\ p)$ we mean $([u],[v]) = \{(x,y):\ x \in [u], y \in [v]\}$.
Since class solutions for the case $p = 2$ are obvious to describe for each of the congruences in the title, throughout the rest of the article we will assume that p is an odd prime number.

Having said that, we start by finding the class solutions for the first the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$, which is more challenging compared to the second congruency $x^2 - y^2 \equiv 0\ (mod\ p)$; and necessary to handle the case of the last one $x^4 - y^4 \equiv 0\ (mod\ p)$. To this end we first point out that in general any congruency of the form $x^n + y^n \equiv 0\ (mod\ p)$ always has the *trivial* class solution $([u], v]) = ([0],[0])$, where class $[0]$ is the class consisting of integer multiples of p.

Evidently here, we are more concerned with finding the existing *non-trivial* solution classes $([u],[v])$ for the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$, where p is an odd prime. Here we first recall that any odd prime number is either of the form $p = 4k - 1$, or else $p = 4k + 1, k = 1, 2, \dots$. This being the case, Proposition 1 bellow shows in the former case $p = 4k - 1$ the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ has only the *trivial* class solution $([0],[0])$, whereas Theorem 1, followed by Proposition 1, shows that in latter case $p = 4k + 1$ the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ has exactly k distinct *primitive* class solutions $([r_i],[s_i]), i = 1, 2, \dots, k$, in the sense defined below.

Definition: For a prime number of the form $p = 4k + 1$, will call the pair $([r],[s])$ a *primitive* class solution for the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ if and r and s are quadratic roots $(mod\ p)$ of the respective quadratic residues a and $p - a\ (mod\ p)$ with $a \in [1, \frac{p-1}{2}]$, and we will refer to such a pair $(a\ ,\ p - a)$ as a pair of least positive complementary quadratic residues $(mod\ p)$.

Note, that any *primitive* class solution $([r],[s])$ defined as above for the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ automatically imply other class solutions derived from quadratic roots r and s. For one thing because of symmetry visible in the congruency $([s],[r])$ will also be another class solution; and what is more for any non-zero integer u, $([us],[ur])$ and $([ur],[us])$ will also be class solutions for the congruency.

hence, to find all *non-trivial* class solutions of the congruency it suffices to find all *primitive* class solution $([r],[s])$ as defined above.

Next, we start with a Lemma regarding the congruency $x^n + y^n \equiv 0\ (mod\ p)$ in general, but later we only use it for $n = 2$ in the proof of the assertion made in upcoming Proposition 1.

Lemma: For a given odd prime number p the congruency $x^n + y^n \equiv 0\ (mod\ p)$ has no *non-trivial* solution with $x^n \equiv y^n\ (mod\ p)$.

Proof: Since the congruency $x^n + y^n \equiv 0\ (mod\ p)$ implies $x^n \equiv -y^n\ (mod\ p)$, if we also have $x^n \equiv y^n\ (mod\ p)$ then it follows that $2x^n \equiv 0\ (mod\ p)$; and this can only happen if $x = mp$, for some m, leading only to the *trivial* solution $([0],[0])$. Hence the he Lemma follows.

The following Proposition 1 implies the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ will have no *non-trivial* solutions when p is of the form $p = 4k - 1, k = 1, 2, n$ ...

Proposition 1: (*Astaneh*) The congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ has *non-trivial* solution(s) if and only if $p \equiv 1\ (mod\ 4)$.

Proof: Assume first that $p \equiv 1\ (mod\ 4)$. That is $p \equiv 4k + 1$ for some $k = 1, 2, \ldots$. Let a be a quadratic residue $(mod\ p)$. Then there is an integer x such that $x^2 \equiv a$. We show that the integer $-a$ is also a quadratic residue $(mod\ p)$. To this end using Legendre's symbol on quadratic residues, we have,

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right).\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}.\left(\frac{a}{p}\right) = (-1)^{2k}.1 = 1,$$

showing that $-a$ is also a quadratic residue $(mod\ p)$.Therefore there exists another integer y such that $y^2 \equiv -a$. Since for the integers x and y the cogruences $x^2 \equiv a$ and $y^2 \equiv -a$ imply $x^2 + y^2 \equiv 0\ (mod\ p)$; proof of the if part of the Proposition follow. "

Remark: The proof just presented also shows when $p \equiv 1\ (mod\ 4)$ quadratic residues $(mod\ p)$ occur in distinct pairs of the integers of the form $(a, p - a)$, where both integers a and $p - a$ can be chosen from the $[1, p - 1]$, and in what follows we will assume this is always. The above proof also implies that the number of quadratic residues $(mod\ p)$ is even; and since the number of quadratic residues $(mod\ p)$ is $\frac{p-1}{2}$ for any prime p, it follows that there are exactly $\frac{\frac{p-1}{2}}{2} = k$ distinct pairs of quadratic residues $(a, p - a)$ with $a, p - a \in [1, p - 1]$. Moreover, there are exactly k pairs of such pair with $a < p - a$; another words, there are exactly k pairs of *least positive complementary* pair of quadratic residues $(mod\ p)$ for the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ "

Next, for the proof of the only if part of the Proposition, assume the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ has *non-trivial* Solution(s). Since by Lemma $x^2 \not\equiv y^2\ (mod\ p)$ the integers $a = x^2$ and $b = y^2$ are distinct quadratic residues $(mod\ p)$. Since we agreed not to distinguish between potential solutions (x, y) and (y, x), without loss of generality we assume $1 \leq a < b \leq p - 1$. We will now choose $a \equiv c\ (mod\ p)$ and $b \equiv d\ (mod\ p)$ such that, say $1 \leq a < b \leq p - 1$. Then on one hand,

$2 \leq a + b \leq 2p - 2$, and on the other hand $a + b \equiv x^2 + y^2 \equiv 0\ (mod\ p)$.
Now since $2 \leq a + b \leq 2p - 2$, it follows that $a + b = p$, or $b = p - a$. This means that quadratic residues $(mod\ p)$ occur in pairs of distinct integers $(a, p - a)$, where both integers a and b are in the interval $[1, p - 1]$. Therefore, there exist an even number of quadratic residues $(mod\ p)$. Since for any odd prime p there are always $\frac{p-1}{2}$ quadratic residues $(mod\ p)$, it follows that $\frac{p-1}{2}$ is an even number. Therefore $\frac{p-1}{2} = 2k$ for some k. Hence $p = 4k + 1$, and the proof of Proposition 1 is complete.

The "*Remark*" made in between the proofs of the if part and the only if part of the above Proposition 1 implies the following Corollary which is used in the upcoming Theorem.

Corollary: For an odd prime number p the quadratic residues $(mod\ p)$ occur in pairs $(a, p - a)$ if and only if $p \equiv 4k + 1, k = 1, 2, \ldots$; this implies that there are exactly k such a pair $(a, p - a)$ least positive complementary of quadratic residues $(mod\ p)$ for which $a < p - a$,; as we have agreed that potential solutions (x, y) and (y, x) are considered the same class solution of the congruency.

In the light of the above Corollary, and in order to describe all possible *non-trivial* solutions of the congruency equation $x^2 + y^2 \equiv 0\ (mod\ p)$ for the case $p \equiv 1\ (mod\ 4)$ in an orderly fashion, here we make certain relevant definitions.

Now, when $p = 4k + 1$ the following Theorem 1 implies that the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ has exactly k distinct *non-trivial* class solutions; moreover the Theorem also describes each one of the k distinct *non-trivial* class solutions in as a pair of square roots $(mod\ p)$ of a *least positive complementary pairs* pair of quadratic residues $mod\ (p)$.

Theorem 1 :(*Astaneh*) Given the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$, where p is an odd prime number;

(a) If $p = 4k - 1, k = 1, 2, \ldots$, the only class solutions of the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ equation is the *trivial* one $([0], [0])$.

(b) If $p = 4k + 1, k = 1, 2, \ldots$. Then, up to multiplication of both components of class solutions $([r], [s])$ by an integer $u \not\equiv 0\ (mod\ p)$, i.e. $(u \times [r], u \times [s])$, the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$ has a further k *non-trivial* primitive class solutions. More precisely for $i = 1, 2, \ldots, k$, if (a_i, b_i) is the ith *least positive complimentary* quadratic residues $(mod\ p)$; and if r_{i0}, and s_{i0} are the respective *least positive quadratic roots* $(mod\ p)$ for a_i and b_i, then $([r_{i0}], [s_{i0}])$ is the ith *non-trivial* class solution of the congruency $x^2 + y^2 \equiv 0\ (mod\ p)$.

Note, that in assertion **(b)**, the set $u \times [r] \subsetneq$ of integers is a proper subset of the class $[u \times r]$. For example, when $u = 2$, the integer $2r + 5p \in [2r]$, but since $2 \times [r] = \{2r + 2kp : k \in \mathbb{Z}\}$, $2r + 5p \notin 2 \times [r]$ as for no $k \in \mathbb{Z}$ we can have $2r + 2kp = 2r + 5p$. Hence $u \times [r] \subsetneq [ur]$, unless of course $u = 1$.

Proof: Part **(a)** follows directly from assertion of Proposition 1.
Part **(b)** simply follows from the Corollary to the Proposition 1, in conjunction with the *Remark* made between the proof of the if part and the only if part of the Proposition 1; together with the fact that for any pair (r_{i0}, s_{i0}) of *least positive*

quadratic roots $(mod\ p)$, corresponding to a pair (a_i, b_i) of *least positive quadratic residues* $(mod\ p)$, we have $r_{i0}^2 + s_{i0}^2 = a_i + b_i = p$.

Example 1 Since $p = 11 = 4 \times 3 - 1$, by part (a) of Theorem 1 the only class solution for the congruency $x^2 + y^2 \equiv 0\ (mod\ 11)$ is the *trivial* one $([0], [0])$.

Example 2 For $p = 13 = 4 \times 3 + 1$, apart from the *trivial* class solution $([u], [v]) = ([0], [0])$, part **(b)** of the Theorem implies that the congruency $x^2 + y^2 \equiv 0\ (mod\ 13)$ has $k = 3$ further class solutions; each defined by one of the three existing pair of *least positive complimentary* quadratic residue $(a_1, b_1) = (1,12)$, $(a_2, b_2) = (3,10)$, and , $(a_3, b_3) = (4,9)$ whose respective *least positive quadratic roots* $(mod\ 13)$ as ordered pairs are $(r_{10}, s_{10}) = (1,5)$, $(r_{20}, s_{20}) = (4,6)$, and $(r_{30}, s_{30}) = (2,3)$. Therefore, up to multiplication by an integer $u \not\equiv 0\ (mod\ 13)$, the 3 further (*non-trivial*) class solutions for congruency $x^2 + y^2 \equiv 0\ (mod\ 13)$ are $([1], [5])$, $([4], [6])$, and $([2], [3])$. Hence all existing class solutions of the congruency $x^2 + y^2 \equiv 0\ (mod\ 13)$ can be described are $(u \times [1], u \times [5])$, $(u \times [4], u \times [6])$, and $(u \times [2], u \times [3])$, with $u \in \mathbb{Z}$ and $u \not\equiv 0\ (mod\ p)$.
Observe that, by the Note following Proof of Theorem 1, since both $([2], [3])$and $([4], [6])$ are primitive solutions, the class solution and $([4], [6])$ can't be ignored as a primitive class solution just because $([2], [3])$ is one, and that $(4,6) \in (2 \times [2], 2 \times [3])$ is a solution of the congruency; simply because $(2 \times [2], 2 \times [3])$ is a subset of $([4], [6])$. More precisely, an example would be that

$$(2 \times 2 + 5 \times 13\ , 2 \times 3 + 5 \times 13) \in ([2], [3])$$

and $$(2 \times 2 + 5 \times 13\ , 2 \times\ 3 + 5 \times 13) \in ([4], [6]),$$

whereas $$(2 \times 2 + 5 \times 13\ , 2 \times\ 3 + 5 \times 13) \notin (2 \times [2], 2 \times [3]).$$

Next, we present class solutions for the easier congruency $x^2 - y^2 \equiv 0\ (mod\ p)$ as the following Proposition 2. Although one can again use quadratic residues $(mod\ p)$ to handle this case, the identity $x^2 - y^2 = (x - y)(x + y)$ suggest the easier method seen in the Proof below. However, a bit of effort is involved to show that class solutions obtained from the two methods are indeed the same.

Proposition 2: Let p be any prime number. Then class solutions of the congruency $x^2 - y^2 \equiv 0\ (mod\ p)$ are,

(a) $([u], [u])$, $u \in \mathbb{Z}$.

(b) $([u], [-u])$, $u \in \mathbb{Z}$.

Proof: It is enough to consider that the congruency $x^2 - y^2 \equiv 0\ (mod\ p)$ is equivalent to the system of two congruences $x - y \equiv 0\ (mod\ p)$ and $x + y \equiv 0\ (mod\ p)$ and the fact that the list in **(a)** represents all class solutions of the former congruency $x - y \equiv 0\ (mod\ p)$, whereas list **(b)** represents all class solutions of the latter congruency $x + y \equiv 0\ (mod\ p)$.

Theorem 2 :(*Astaneh*) Given the congruency $x^4 - y^4 \equiv 0\ (mod\ p)$, where p is an odd prime number;

(a) If $p = 4k - 1, k = 1, 2, ...$, then the only class solutions of the congruency $x^4 - y^4 \equiv 0\ (mod\ p)$ are of the form $([u], [u])$, $u \in \mathbb{Z}$ together with those of the form $([u], [-u])$, $u \in \mathbb{Z}$.

(b) If $p = 4k + 1, k = 1, 2, ...$, then class solutions of $x^4 - y^4 \equiv 0\ (mod\ p)$ are

(i) All class solutions $([u],[u])$, $u \in \mathbb{Z}$ and $([u],[-u])$, $u \in \mathbb{Z}$.
(j) All class solutions listed in part **(b)** of Theorem 1.

Proof : Since the congruency $x^4 - y^4 \equiv 0\ (mod\ p)$ is equivalent to the system of two congruences $(x-y)(x+y) \equiv 0\ (mod\ p)$ and $x^2 + y^2 \equiv 0\ (mod\ p)$, and since by Proposition 2 class solutions of the former congruency of the is as listed in part **(i)** , and because $p = 4k + 1$ implies class solutions of the latter congruency are the ones listed in part **(b)** of Theorem 1, the proof is complete.

Example 3 Since $p = 11 = 4 \times 3 - 1$, by Proposition 2 class solution for the congruency $x^4 - y^4 \equiv 0\ (mod\ 11)$ are all $([u],[u])$, $u \in \mathbb{Z}$ and $([u],[-u])$, $u \in \mathbb{Z}$.

Example 4 For $p = 13$, Proposition 2 implies class solutions of the congruency $x^4 - y^4 \equiv 0\ (mod\ 13)$ include all $([u],[u])$ and $([u],[-u])$, $u \in \mathbb{Z}$, and since $13 = 4 \times 3 + 1$, as seen in Example 2, part **(b)** of Theorem 1 implies that the only remaining class solutions of the congruency $x^4 - y^4 \equiv 0\ (mod\ 13)$ are $([1],[5])$, $([4],[6])$, and $([2],[3])$.